500.42806X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): A. OKUYAMAI, et al

Serial No.:

Filed: June 24, 2003

Title: INFORMATION RECORDING/REPRODUCING SYSTEM

Group:

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

June 24, 2003

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2002-182325 filed June 24, 2002.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Melvin Kraus
Registration No. 22,466

MK/nac
Attachment
(703) 312-6600

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　６月２４日

出願番号
Application Number: 特願２００２－１８２３２５

[ST.10/C]: [ＪＰ２００２－１８２３２５]

出願人
Applicant(s): 株式会社日立製作所

２００３年　４月　８日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０２４３５２

【書類名】　特許願

【整理番号】　1502001481

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 13/36

【発明者】

【住所又は居所】　茨城県土浦市神立町５０２番地　株式会社　日立製作所機械研究所内

【氏名】　奥山　淳

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　道明　誠一

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　小川　仁

【発明者】

【住所又は居所】　茨城県土浦市神立町５０２番地　株式会社　日立製作所機械研究所内

【氏名】　薄井　和明

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【電話番号】　03-3212-1111

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】情報記録再生システム

【特許請求の範囲】

【請求項１】

情報を記録再生する磁気ディスク装置と、該磁気ディスク装置を着脱可能に接続し該磁気ディスク装置に対して情報の記録再生のためのアクセスを行なうホストシステムとを有する情報記録再生システムにおいて、

前記磁気ディスク装置は、自身の物理的な特性に基づき認証鍵を作成する認証鍵作成手段を有することを特徴とする情報記録再生システム。

【請求項２】

前記磁気ディスク装置及び前記ホストシステムは、前記認証鍵を記録する認証鍵記録手段をそれぞれ有すると共に、前記認証鍵に基づき認証データを作成する認証データ作成手段をそれぞれ有し、前記ホストシステムの認証データと、前記磁気ディスク装置の認証データとに基づいて、前記ホストシステムからの前記磁気ディスク装置の情報へのアクセスを制御するアクセス制御手段を少なくとも一つ有することを特徴とする請求項１に記載の情報記録再生システム。

【請求項３】

前記認証鍵は、前記磁気ディスク装置が有する磁気ディスクの媒体欠陥特性に基づき作成することを特徴とする請求項１に記載の情報記録再生システム。

【請求項４】

前記認証鍵は、前記磁気ディスク装置が有する磁気ディスクの偏心特性に基づき作成することを特徴とする請求項１に記載の情報記録再生システム。

【請求項５】

前記認証鍵は、前記磁気ディスク装置が有する磁気ディスクの偏心特性を補償する偏心補償信号に基づき作成することを特徴とする請求項１に記載の情報記録再生システム。

【請求項６】

前記認証鍵は、前記磁気ディスク装置が有する磁気ディスクの偏心特性を補償する偏心補償信号をウェーブレット変換した結果に基づき作成することを特徴とす

る請求項１に記載の情報記録再生システム。

【請求項７】

前記認証鍵は、３個所以内のそれぞれ異なるシリンダで作成された偏心補償信号に基づき作成することを特徴とする請求項１に記載の情報記録再生システム。

【請求項８】

前記磁気ディスク装置は、前記磁気ディスク装置が有する磁気ディスクの偏心を補償する偏心補償信号を作成する手段と、前記認証鍵に基づき前記偏心補償信号を暗号化する手段と、暗号化された前記偏心補償信号を記録する手段と、暗号化された前記偏心補償信号を前記認証鍵に基づき暗号化前の偏心補償信号に戻す手段とを有することを特徴とする請求項１に記載の情報記録再生システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報を記録再生する磁気ディスク装置とこの磁気ディスク装置を着脱可能に接続してアクセスを行なうホストシステムとを有する情報記録再生システムに関し、磁気ディスク装置にアクセスするホストシステムを特定のものに限定可能とする情報記録再生システムに関する。

【０００２】

【従来の技術】

磁気ディスク装置をホストシステムから着脱可能にして、音楽サーバ、ビデオレコーダ、携帯情報端末、カーナビゲーションなどで動画や音声といったデータを記録再生する用途として使用するシステムが提案されている。着脱可能な構成であるため、第三者が不当に磁気ディスク装置を取り外し、別のホストシステムで情報を読み書きする等のセキュリティ上の問題が考えられる。磁気ディスク装置とホストシステムの組み合わせを限定する技術としては、認証データを用いた相互認証処理がある。例えば、特開２００１－２５６００４号公報では、記憶装置或いはホストシステムの一方で作成された認証データに基づいて他方がアクセス制御用の認証データを作成し、この認証データを用いてホストシステムのアクセス制御を行なう技術を開示している。認証データは、記憶装置或いはホストシ

ステムの固有情報と日時情報に基づいて作成される。固有情報としては、メーカ名、機種名、シリアル番号を使用している。

【０００３】

【発明が解決しようとする課題】

特開２００１－２５６００４号公報の技術では、容易に入手できる情報を用いているため、認証鍵を予測できる可能性がある。また、不正なユーザによって、ある１つの装置から認証鍵を取得されてしまった場合、メーカ名、機種名、シリアル番号に基づき別の装置の認証鍵も容易に予測できる可能性がある。

【０００４】

本発明の目的は、予測が困難な認証鍵によって相互認証を行うことにより、磁気ディスク装置とホストシステムとを特定の組み合わせに限定することが可能なシステムを提供することにある。

【０００５】

【課題を解決するための手段】

本発明の情報記録再生システムは、磁気ディスク装置及びホストシステムの各々の認証鍵記憶手段に、磁気ディスク装置の物理的な特性に基づき作成する認証鍵を記録する。認証鍵は、例えば磁気ディスク装置が有する磁気ディスクの媒体欠陥特性或いは偏心特性に基づいて作成するとよい。更に、磁気ディスク装置及びホストシステムは、前記認証鍵を使用して認証データを作成する。そして、磁気ディスク装置のアクセス制御手段において、ホストシステムで作成された認証データと、磁気ディスク装置で作成された認証データとに基づいて、磁気ディスク装置へのアクセスを特定のホストシステムのみに限定するよう制御する。或いは、ホストシステムのアクセス制御手段において、磁気ディスク装置で作成された認証データと、ホストシステムで作成された認証データとに基づいて、ホストシステムを特定の磁気ディスク装置のみに限定してアクセスを行うように制御する。

磁気ディスクの媒体欠陥特性或いは偏心特性の発生は、人間の手が介在していない。また、それぞれの磁気ディスク装置毎に特性が異なる。従って、磁気ディスクの媒体欠陥特性或いは偏心特性から作成される認証鍵は、人間の指紋のよう

にそれぞれの磁気ディスク装置毎に異なり、予測は極めて困難である。

【０００６】

【発明の実施の形態】

以下、本発明の実施形態について図面を用いて説明する。

【０００７】

図１は、本発明の実施形態による情報記録再生システムの構成図の一例である。本情報記録再生システムは、磁気ディスク装置１００とホストシステム１０１とからなる。磁気ディスク１は、スピンドルモータ（ＳＰＭ）２により回転される。なお、磁気ディスク１の各トラック（図示せず）には、サーボ情報が記録されたサーボ領域と、データを記録するためのデータ領域とを有する。磁気ヘッド３は、アクチュエータ４に搭載されて、磁気ディスク１の半径方向に移動される。アクチュエータ４はボイスコイルモータ（ＶＣＭ）５を駆動源として構成されている。ＳＰＭ２及びＶＣＭ５は、後述するＣＰＵ９の制御により、ＶＣＭ／ＳＰＭドライバ６から駆動電流を供給されて駆動する。ＶＣＭ／ＳＰＭドライバ６は、通常ではＣＰＵ９からゲートアレイ７を介してディジタル制御値を入力し、当該制御値に応じて駆動電流を出力する。リード／ライト回路（Ｒ／Ｗ回路）８は、磁気ヘッド３の信号からリード信号を復調したり、磁気ヘッド３にライト信号を供給する。なお、Ｒ／Ｗ回路８は、サーボ情報から磁気ヘッド３の位置を検出する位置検出回路（図示せず）を有する。ＨＤＣ１２は、ホストシステム１０１との間でのデータ転送を制御するものであり、ホストシステム１０１から入力されるデータを一時的にランダムアクセスメモリ（ＲＡＭ）１１に記憶させる等といった制御を行なう。セントラルコントロールユニット（ＣＰＵ）９は、リードオンリーメモリ（ＲＯＭ）１０に格納された制御プログラムに従って、アクチュエータの制御等を行なう。１３は認証鍵作成手段、１４は認証鍵記録手段、１５は認証データ作成手段、１６はアクセス制御手段である。これらの詳細については後述する。ゲートアレイ７、Ｒ／Ｗ回路８、ＣＰＵ９、ＲＯＭ１０、ＲＡＭ１１、ＨＤＣ１２、認証鍵作成手段１３、認証鍵記録手段１４、認証データ作成手段１５、アクセス制御手段１６は、それぞれバスで接続されている。本実施形態の磁気ディスク装置１００は、従来の磁気ディスク装置と言われている情報を

磁気ディスクに記録再生する情報記録再生部に加えて、認証鍵作成手段１３、認証鍵記録手段１４、認証データ作成手段１５、アクセス制御手段１６とを備えたものである。

【０００８】

１７はインターフェース（Ｉ／Ｆ）回路、１８はＣＰＵ、１９はＲＯＭ、２０はＲＡＭ、２１は認証鍵記録手段、２２は認証データ作成手段、２３はアクセス制御手段である。なお、ホストシステム１０１は、パーソナルコンピュータ、音楽サーバ、ビデオレコーダ、携帯情報端末、カーナビゲーションなどを想定しており、必ずしも上記の各要素の全てを含まなくとも良い。

次に、認証鍵作成手段１３の一例について説明する。通常、磁気ディスク装置の記録再生処理は、記録媒体である磁気ディスクのデータ記録領域に設定されたセクタを最小単位として行われる。このとき、磁気ディスクのデータ記録領域に設定された多数のセクタの中には、磁気ディスクに付着した塵埃や組み立て工程時の損傷等の影響を受けて、データの書き込みや読み出しが正常に行なわれないセクタが存在する場合がある。このようなセクタは欠陥セクタと呼ばれている。磁気ディスクに記録するデータの信頼性を確保する上では、上記のような欠陥セクタを適切に検出して、この欠陥セクタにはデータの記録を行なわないことが望まれる。そこで、磁気ディスクに対してデータの記録再生を行なう際は、一般に、ディフェクト管理と呼ばれる欠陥セクタを管理するための処理が行われている。

【０００９】

磁気ディスク上に発生する欠陥は、磁気ディスク初期化の際に発見される１次欠陥と、磁気ディスクへのデータ記録終了後に記録したデータを再度読み取りして正しい記録が行われたかを判定するいわゆるベリファイを行なった際に発見される２次欠陥とに分けられる。ディフェクト管理を行なう場合、磁気ディスクのデータ記録領域には、欠陥セクタについての情報をテーブル化して書き込んでおくためのディフェクト管理エリア（ＤＭＡ）と呼ばれる領域が設けられる。そして、欠陥セクタが検出された場合には、この欠陥セクタの位置情報等がこのＤＭＡに書き込まれる。一般に、１次欠陥はＤＭＡのＰＤＬ（Ｐｒｉｍａｒｙ　Ｄｅ

ｆｅｃｔ　Ｌｉｓｔ）と呼ばれる部分に書き込まれ、２次欠陥はＤＭＡのＳＤＬ（Ｓｅｃｏｎｄａｒｙ　Ｄｅｆｅｃｔ　Ｌｉｓｔ）と呼ばれる部分に書き込まれる。

【００１０】

図２に、欠陥セクタ情報の位置を表す欠陥配置図の一例を示す。縦軸は磁気ヘッドのヘッド番号、横軸は磁気ディスク装置のセクタ番号である。図２では、磁気ヘッドのヘッド番号を０～３とし、セクタ番号を０～５としている。なお、今後、図２のテーブルの各要素の場所は、（ヘッド番号、セクタ番号）のようにヘッド番号とセクタ番号の指定で表すことにする。欠陥セクタが検出されない場合は、（０、０）から（０、５）までのテーブルに、論理値０～５を格納する。次に、（１、０）から次の論理値６を格納して行く。欠陥セクタが検出された場合は、欠陥の種類を区別できる情報を格納する。欠陥の種類としては、欠陥部分を飛ばして追従するスリップディフェクトと、欠陥を他のテーブルに移動させる交代ディフェクトが存在する。スリップディフェクトは、図２の（１、１）と（２、５）に示すように、先頭にＳを付加する。交代ディフェクトは、図２の（２、３）に示すように、先頭にＲを付加する。また、欠陥の番号は、論理値の順に１から付加する。

【００１１】

図３に、欠陥管理テーブルの一例を示す。図３は、図２の欠陥配置図から各欠陥のヘッド番号とセクタ番号を抜き出して表示したものである。スリップディフェクトであるＳ１とＳ３は、その情報が格納されているヘッド番号とセクタ番号を示している。交代ディフェクトであるＲ２は、元の位置のヘッド番号とセクタ番号、移動先のヘッド番号とセクタ番号を示している。

【００１２】

認証鍵を、上記欠陥管理テーブルを基に作成する。図４に、認証鍵作成の手順を示すフローチャートの一例を示す。ホストシステム１０１から認証鍵作成の要求コマンドを受け取った場合（２００）、欠陥管理テーブルを基に認証鍵を作成する（２０１）。欠陥管理テーブルから値を選択し、２進数に変換し、例えば２５６ビット以内の５６ビットや１２８ビットの認証鍵を作成する。欠陥管理テー

ブル値の選択は、どのような規則に従って選んでもかまわない。また、欠陥管理テーブル値を、ＤＭＡのＰＤＬだけから読み出すことにして、１次欠陥の値だけから選ぶことも可能である。更にまた、後述する認証データ作成手段１５、２２で認証データを作成する際に必要とする認証鍵の数に合わせて、複数の認証鍵を作成することも可能である。

【００１３】

作成した認証鍵は、ホストシステム１０１に送信するとともに（２０２）、認証鍵記録手段１４に記録する（２０３）。また、ホストシステム１０１は、受信した認証鍵を認証鍵記録手段２１に記録する。欠陥の特徴として、磁気ディスク装置毎に欠陥の種類や場所が異なっているということが上げられる。また、欠陥の発生に人間の手が介在していないということが上げられる。従って、複製は不可能であり、不正な改ざん等に対して強固な認証鍵として使用できる。更に、今後、磁気ディスク装置の記録密度が向上し、データ記録密度が向上するほど欠陥の数は増加すると考えられる。従って、磁気ディスク装置の記録密度向上に対応して、不正な改ざん等に対してより強固な認証鍵を作成することが可能となる。

【００１４】

次に、認証鍵作成手段１３の別の一例について説明する。通常、磁気ヘッドを追従させるべき磁気ディスク上のトラックには、特にディスクの回転に伴う要因により偏心が発生する。要因としては、磁気ディスクを回転させるためのＳＰＭの軸振れ、サーボ情報を書き込む時の磁気ディスクの振動等がある。また、磁気ディスク上にサーボ情報を書き込む時に、磁気ディスクを実装する磁気ディスク装置自体ではなく、サーボライタと呼ばれる専用のサーボ情報書き込み装置を使用することがある。このような場合には、サーボ情報を書き込みした磁気ディスクを磁気ディスク装置に装着した時に、ＳＰＭの回転中心と、サーボライタによりサーボ情報を書き込みした時の磁気ディスクの取り付け位置での回転中心との誤差により、巨大な偏心が発生する可能性がある。このようなトラック偏心に伴う振幅は、磁気ヘッドの位置誤差量に換算して、数十μｍ程度になることもある。なお、ディスク偏心特性は、１台の磁気ディスク装置でもトラック毎に特性が異なる。

【００１５】

高トラック密度化を図る磁気ディスク装置では、確実にデータを記録再生するための誤差の許容範囲は０。数μｍ程度である。誤差がこの許容範囲を越える場合には、磁気ヘッドを目標トラックに追従させることが困難となる。そのため、一般的に、ディスク偏心特性を検出して偏心による位置誤差を低減する偏心補償信号を作成し、ヘッド位置決め制御系において偏心の影響を補償している。偏心補償信号を作成する方法は、繰り返し制御に基づく方法、フーリエ級数展開に基づく方法、外乱オブザーバに基づく方法等、多くの方法が提案されている。偏心補償は、リアルタイムに偏心補償を行う方式と、偏心補償信号に基づき予めテーブルを作成しておき、サーボセクタ番号に基づきテーブル値を読み出すテーブル参照方式とに大別できる。ただし、磁気ディスクの回転周波数の数倍程度の低次の偏心特性は、周囲環境温度などの使用条件の影響を受けて、変動する場合が考えられる。そこで、一般的には、低次の偏心はリアルタイムに偏心補償信号を作成して補償される。

【００１６】

認証鍵を、上記偏心補償信号を基に作成する。図５に、ヘッド位置決め制御系のブロック線図の一例を示す。また、図６に、認証鍵作成の手順を示すフローチャートの一例を示す。ヘッド位置決め制御系は、磁気ヘッド３が読み出したサーボ情報から検出される磁気ヘッド３の位置信号に基づき、フィードバック制御系が構成されている。それぞれ具体的には、制御対象は図１のＶＣＭ５等から構成される磁気ヘッド３の移動機構であり、コントローラ、第１の偏心補償手段、第２の偏心補償手段、平均化手段はＣＰＵ９で演算されるプログラム或いはハードロジックである。また、記憶手段は、ＲＯＭ１０やＲＡＭ１１等のメモリであればよく、或いは磁気ディスク１の特定の記録領域とすることも可能である。特定の記憶領域とは、通常のデータの記録動作では書き換え不可能（アクセス不可能）な例えば代替セクタ（冗長記録領域）やサーボ領域を想定する。

【００１７】

変動する場合が考えられる低次の偏心特性はリアルタイムに第１の偏心補償手段で補償し、それ以外の偏心特性は第２の偏心補償手段によりテーブル参照方式

で補償する。ただし、第２の偏心補償信号は、例えばディスク４回転分の第２の偏心補償信号の同一サーボセクタ番号の値に対して平均化処理を行い、記憶手段に記憶する。このとき、ノイズ対策等の目的でフィルタ処理を併用してもよい。平均化された第２の偏心補償信号は、サーボセクタ番号に基づき読み出される。偏心補償手段は、偏心補償信号を作成することができるのならば、どのような方法でもかまわない。また、操作信号に基づき偏心補償信号を作成し、作成した偏心補償信号を操作信号に加算する方式でも同様な手順で行うことができる。

【００１８】

ホストシステム１０１から認証鍵作成の要求コマンドを受け取った場合（３００）、目標シリンダとヘッド番号を設定し（３０１）、シークを行う（３０２）。次に、目標シリンダにシーク後、第１の偏心補償信号の過渡特性が収束するまで例えばディスク４回転分待ち、その後、平均化された第２の偏心補償信号を作成する（３０３）。次に、平均化された第２の偏心補償信号を基にして、周囲環境温度などの使用条件の影響を受けない高次成分を取り出すための処理を行う。例えば、ハイパスフィルタ処理を行い第２の偏心補償信号から高次成分を取り出す。なお、フィルタ特性は、位相が０或いは群遅延特性が一定であることが望ましい。また、ウェーブレット変換を行い第２の偏心補償信号から高次成分を取り出す。例えば、多重解像度解析を行ない、第１回目のウェーブレット分解のハイパス要素を用いてもよい。更に、第２回目以降のウェーブレット分解結果を用いてもよい。また、ウェーブレットパケット解析を行ない、第１回目のウェーブレットパケット分解のハイパス要素を用いてもよい。更に、第２回目以降のウェーブレットパケット分解結果を用いてもよい。

【００１９】

３０１から３０４までの処理は、適当な回数だけ行う（３０５）。例えば、１トラックにサーボセクタ数が１００個の場合、３０１から３０４までの処理を目標シリンダを変えながら３回行うことにより、３００個の平均化された第２の偏心補償信号値が作成される。この３００個の平均化された第２の偏心補償信号値から値を選択し、２進数に変換し、例えば２５６ビット以内の５６ビットや１２８ビットの認証鍵を作成する（３０６）。目標シリンダの選択は、どのような規

則に従って選んでもかまわない。また、２進数に変換する値の選択は、どのような規則に従って選んでもかまわない。更にまた、後述する認証データ作成手段１５、２２で認証データを作成する際に必要とする認証鍵の数に合わせて、複数の認証鍵を作成することも可能である。

【００２０】

作成した認証鍵は、ホストシステム１０１に送信するとともに（３０７）、認証鍵記録手段１４に記録する（３０８）。また、ホストシステム１０１は、受信した認証鍵を認証鍵記録手段２１に記録する。

【００２１】

偏心の特徴として、磁気ディスク装置毎に特性が異なっているということが上げられる。また、偏心の発生に人間の手が介在していないということが上げられる。従って、複製は不可能であり、不正な改ざん等に対して強固な認証鍵として使用できる。更に、今後、磁気ディスク装置の記録密度が向上し、トラック密度が向上するほどサーボセクタ数は増加すると考えられる。従って、磁気ディスク装置の記録密度向上に対応して、不正な改ざん等に対してより強固な認証鍵を作成することが可能となる。

【００２２】

これらの認証鍵は、認証鍵記録手段１４と２１に記録される。認証鍵記録手段１４と２１は、ＲＯＭ等のメモリであれば良い。なお、認証鍵記録手段１４をＲＯＭ１０で代用し、認証鍵記録手段２１をＲＯＭ１９で代用することも可能である。更に、磁気ディスク１の特定の記録領域に記録することも可能である。特定の記憶領域とは、通常のデータの記録動作では書き換え不可能（アクセス不可能）な例えば代替セクタ（冗長記録領域）やサーボ領域を想定する。これらを併用することにより、改ざん等に対してより強固な認証鍵とすることも可能である。

【００２３】

図４或いは６の手順で認証鍵を作成する時期としては、組み合わせを限定する目的で磁気ディスク装置がホストシステムに装着されたときに認証鍵を作成してもよい。例えば、磁気ディスク装置側に初めて認証鍵を作成すると１になるフラグを用意する。すなわち、１度でも認証鍵を作成したことがある場合は、それ以

後上記フラグは１のままになる。このフラグは、通常のデータの記録動作では書き換え不可能（アクセス不可能）な例えば代替セクタ（冗長記録領域）やサーボ領域に作成されることが望ましい。

【００２４】

ホストシステムは、磁気ディスク装置が装着されたときに、磁気ディスク装置に上記フラグ情報を確認してその結果を送信するように要求し、上記フラグが０の場合は磁気ディスク装置に認証鍵を作成して送信することを要求するコマンドを送信する。また、組み合わせを限定する目的で磁気ディスク装置がホストシステムに装着されたとき、例えばユーザにより、ホストシステムに認証鍵の作成を要求するコマンドを入力させてもよい。

【００２５】

ホストシステムは、認証鍵の作成を要求するコマンドが入力された場合、磁気ディスク装置に認証鍵を作成して送信することを要求するコマンドを送信する。この際、例えば、ホストシステム側でユーザからの認証鍵作成要求の回数を管理して、ユーザが認証鍵の作成を要求できる回数に制限を持たせておくことが望ましい。更にまた、磁気ディスク装置とホストシステムとを有する情報記録再生システムを停止する際、認証鍵を作成してもよい。

【００２６】

ホストシステムが停止命令を受けた場合、磁気ディスク装置に認証鍵を作成して送信することを要求するコマンドを送信する。この際、例えば、ホストシステム側から認証鍵の受信完了を示すフラグを磁気ディスク装置に送信し、磁気ディスク装置はそのフラグを受信してから停止し、ホストシステムはフラグ送信後から磁気ディスク装置が停止完了する一定時間経過後に停止することが望ましい。この場合、次回起動時における認証鍵は、前回稼動中に欠陥特性或いは偏心特性が何らかの理由により変化したとしても、その変化を反映した値に更新されている。また、起動毎に異なる認証鍵を用いることになり、不正な改ざん等に対してより強固となる。

【００２７】

次に、磁気ディスク装置１００とホストシステム１０１の認証手順について説

明する。図７は、ホストシステム１０１側から磁気ディスク装置１００の認証を行なう手順を示すフローチャートの一例である。図８は、ホストシステム１０１から認証開始のコマンドを受信した場合の磁気ディスク装置１００側の手順を示すフローチャートの一例である。

【００２８】

まず、ホストシステム１０１側の手順について説明する。ホストシステム１０１は、認証開始を示すコマンドを磁気ディスク装置１００に送信する（４０１）。次に、認証データの元になるデータを作成し（４０２）、磁気ディスク装置１００に送信する（４０３）。このデータは、適当なランダムデータであればよい。次に、このデータを、ホストシステム１０１が有する認証鍵を使って暗号化し（４０４）、磁気ディスク装置１００から暗号文が送られてくるまで待機する（４０５）。磁気ディスク装置１００から暗号文を受信したら、ホストシステム１０１の暗号文と磁気ディスク装置１００の暗号文を比較し（４０６）、一致すれば磁気ディスク装置１００の認証成立とし（４０７）、一致しなければ磁気ディスク装置１００の認証不成立とする（４０８）。

【００２９】

次に、磁気ディスク装置１００側の手順について説明する。認証開始のコマンド入力を受信した場合（５００）、ホストシステム１０１から送られてくるデータを受信する（５０１）。次に、５０２から５０７までの手順により、認証鍵を作成する。この手順は、図６の３０１から３０６までの手順と同様であるので説明は省略する。なお、５０２から５０７までの手順に変わり、欠陥特性に基づく認証鍵を使用する場合などは、認証鍵記録手段１４に記録された認証鍵を読み出す手順としてもよい。

【００３０】

次に、認証鍵を使ってデータを暗号化し（５０８）、ホストシステム１０１に暗号文を送信する（５０９）。これにより、４０６で暗号文が一致すれば、ホストシステム１０１と磁気ディスク装置１００は同一の暗号鍵を有していることになるので認証が成立する。また、磁気ディスク装置１００をホストシステム１０１と読み替えて図７の処理を磁気ディスク装置１００側で行ない、ホストシステ

ム１０１を磁気ディスク装置１００と読み替えて図８の処理をホストシステム１０１側で行なえば、磁気ディスク装置１００側からホストシステム１０１を認証することができる。この場合、５０２から５０７までの手順は、認証鍵記録手段２１に記録された認証鍵を読み出す手順となる。なお、上記で、認証鍵を使ってデータを暗号化する処理は、認証データ作成手段１５と２２で行なっている。

【００３１】

また、暗号文の比較を行なうことにより認証の成立、不成立を判断する処理は、アクセス制御手段１６と２３で行なっている。認証データ作成手段１５と２２は、認証鍵を利用してデータを暗号化できるものであればどのようなものでもかまわない。また、アクセス制御手段１６と２３は、暗号文の比較を行ない、同一かどうかを判断できるものであればどのようなものでもかまわない。例えば、暗号文を２進数に変換して論理積を計算し、結果が１であれば暗号文は一致している。

【００３２】

磁気ディスク装置１００側でホストシステム１００の認証が成立した場合はホストシステム１０１からのアクセスを許可し、認証が不成立の場合はホストシステム１０１からのアクセスを不許可にする。また、ホストシステム１０１側で磁気ディスク装置１００の認証が成立した場合は磁気ディスク装置１００にアクセスを行なえるようにし、認証が不成立の場合は磁気ディスク装置１００にアクセスを行なわないようにする。また、ホストシステム１０１側で磁気ディスク装置１００の認証が不成立の場合は、その旨をユーザに通知してもよい。この相互認証により、ホストシステム１０１と磁気ディスク装置１００の組み合わせを限定することができる。

【００３３】

次に、ホストシステム１０１と磁気ディスク装置１００の組み合わせを限定する別の一例について説明する。図９に、ヘッド位置決め制御系のブロック線図の一例を示す。また、図１０に、第２の偏心補償信号の作成手順を示すフローチャートの一例を示す。

【００３４】

図９は、図５のヘッド位置決め制御系のブロック線図に対して、暗号化手段と復号化手段を加えたものである。まず、ホストシステム１０１から第２の偏心補償信号の作成を要求するコマンドを受信した場合（６００）、目標シリンダを設定し（６０１から６０３）、シークを行なう（６０４）。次に、目標シリンダで平均化された第２の偏心補償信号を作成する（６０５）。次に、作成した第２の偏心補償信号を認証鍵を使って暗号化し（６０６）、記憶する（６０７）。ここまでの処理を、全てのシリンダで行う（６０８）。記憶した第２の偏心補償信号を使用する場合は、復号化手段で認証鍵を利用して暗号化前の第２の偏心補償信号に戻して使用する。ただし、復号化手段で使用する認証鍵は、ホストシステム１０１から受信した認証鍵を用いる。従って、磁気ディスク装置１００は、ホストシステム１０１から正しい認証鍵を受信しない限り、第２の偏心補償信号を利用することができない。そこで、例えば、磁気ディスク装置とホストシステムとを有する情報記録再生システムの起動時に、ホストシステムから磁気ディスク装置に認証鍵を送信するようにする。こうすることにより、同一の認証鍵を有するホストシステムと磁気ディスク装置の組み合わせでない限り、磁気ディスク装置は正しい第２の偏心補償信号を利用できないのでヘッド追従誤差が増加し、正常な記録再生動作を行なうことができない。従って、ホストシステム１０１と磁気ディスク装置１００の組み合わせを限定することができる。

【００３５】

なお、上記本実施形態では、磁気ディスク装置１００のインターフェースとして、ＡＴＡ（ＡＴ　ＡＴＴＡＣＨＭＥＮＴ）規格を想定している。しかし、例えば、ＳＣＳＩ（Ｓｍａｌｌ　Ｃｏｍｐｕｔｅｒ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｆａｃｅ）等にも適用可能である。ホストシステム１０１から例えば認証鍵の取得は、ＡＴＡ規格を利用して行っても良いし、その他の方法で行っても良い。ＡＴＡ規格を利用する一例としては、Ｓｅｔ　Ｆｅａｔｕｒｅｓコマンド（或いはＩｄｅｎｔｉｆｙ　Ｄｅｖｉｃｅコマンド）を利用して認証鍵の取得を行う。ＡＴＡ規格で規定されている同コマンドに対して、例えばベンダユニーク領域或いはリザーブ領域に認証鍵の送信開始を示すビットを設ける。ホストシステム１０１（或いは磁気ディスク装置１００）はＳｅｔ　Ｆｅａｔｕｒｅｓコマンド（或いは

Ｉｄｅｎｔｉｆｙ　Ｄｅｖｉｃｅコマンド）の発行と認証鍵の送信を示すビットを監視していて、例えばビットが１の場合は、磁気ディスク装置１００（或いはホストシステム１０１）に認証鍵を送信する。

【００３６】

以上説明したように、磁気ディスク装置１００とホストシステム１０１との間で、磁気ディスク装置の物理的な特性に基づき作成する認証データを用いて互いの認証を行うようにしたため、磁気ディスク装置側においては、当該磁気ディスク装置へのアクセスを特定のホストシステムのみに限定するように制御でき、また、ホストシステム側においては、特定の磁気ディスク装置のみに限定してアクセスを行うように制御することが可能となる。

【００３７】

【発明の効果】

以上、本発明では、磁気ディスク装置の物理的な特性に基づいて認証データを作成することにより、認証データの予測が極めて困難であり、このような認証データを用いて相互認証を行うことにより、磁気ディスク装置とホストシステムとを特定の組み合わせに限定することが可能である。

【図面の簡単な説明】

【図１】　本発明の実施形態による情報記録再生システムの構成図である。

【図２】　欠陥配置図の一例である。

【図３】　欠陥管理テーブルの一例である。

【図４】　認証鍵の作成手順を示すフローチャートの一例である。

【図５】　ヘッド位置決め制御系のブロック線図の一例である。

【図６】　認証鍵の作成手順を示すフローチャートの一例である。

【図７】　認証処理の手順を示すフローチャートの一例である。

【図８】　認証処理の手順を示すフローチャートの一例である。

【図９】　ヘッド位置決め制御系のブロック線図の一例である。

【図１０】　第２の偏心補償信号の作成手順を示すフローチャートの一例である。

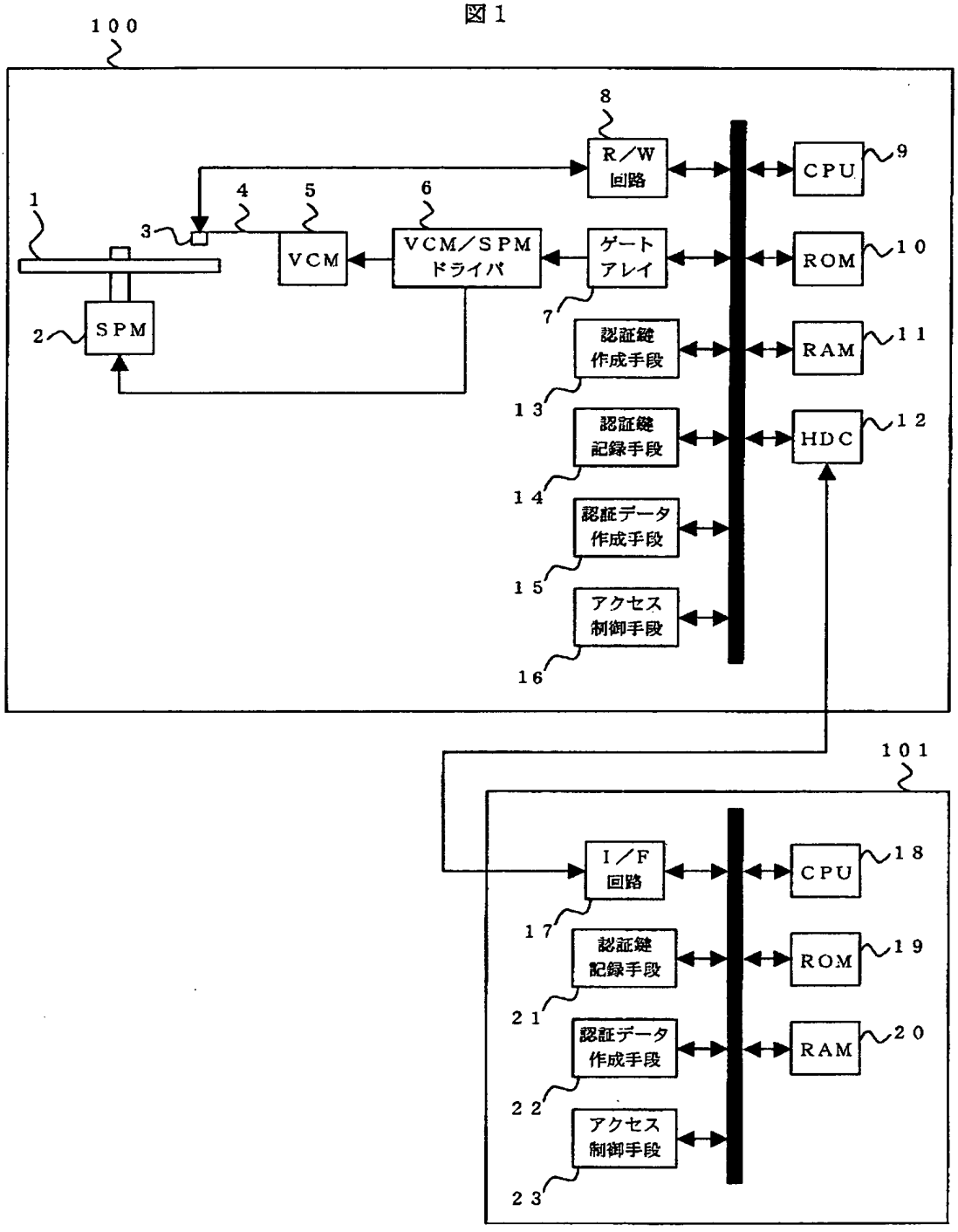
【符号の説明】

１…磁気ディスク、２…ＳＰＭ、３…磁気ヘッド、４…アクチュエータ、５…ＶＣＭ、６…ＶＣＭ／ＳＰＭドライバ、７…ゲートアレイ、８…Ｒ／Ｗ回路、９…ＣＰＵ、１０…ＲＯＭ、１１…ＲＡＭ、１２…ＨＤＣ、１３…認証鍵作成手段、１４…認証鍵記録手段、１５…認証データ作成手段、１６…アクセス制御手段、１７…Ｉ／Ｆ回路、１８…ＣＰＵ、１９…ＲＯＭ、２０…ＲＡＭ、２１…認証鍵記録手段、２２…認証データ作成手段、２３…アクセス制御手段。

【書類名】　図面

【図１】

図１



出証特２００３－３０２４３５２

【図２】

図２

セクタ番号 / ヘッド番号	0	1	2	3	4	5
0	0	1	2	3	4	5
1	6	S１	7	8	9	１０
2	１１	１２	１３	R２	１５	S３
3	１６	１７	１８	１９	１４	SP

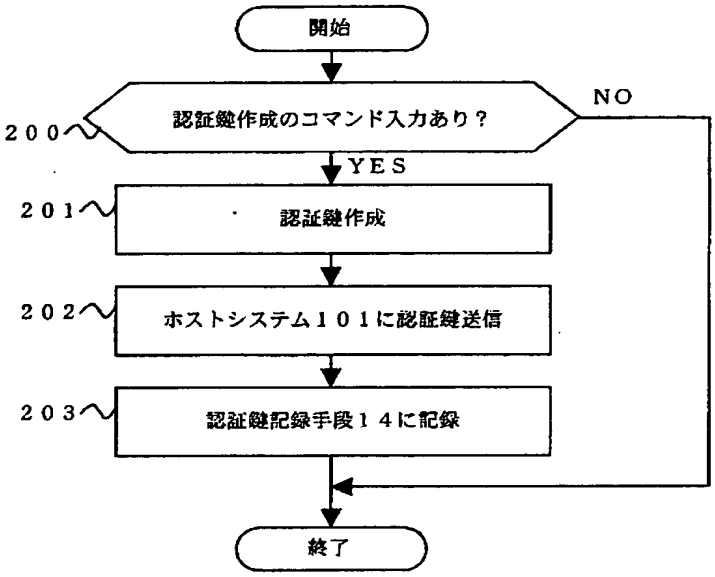
【図３】

図３

S１	ヘッド番号	1
	セクタ番号	1
R２	１次ヘッド	2
	１次セクタ	3
	２次ヘッド	3
	２次セクタ	4
S３	ヘッド番号	2
	セクタ番号	5

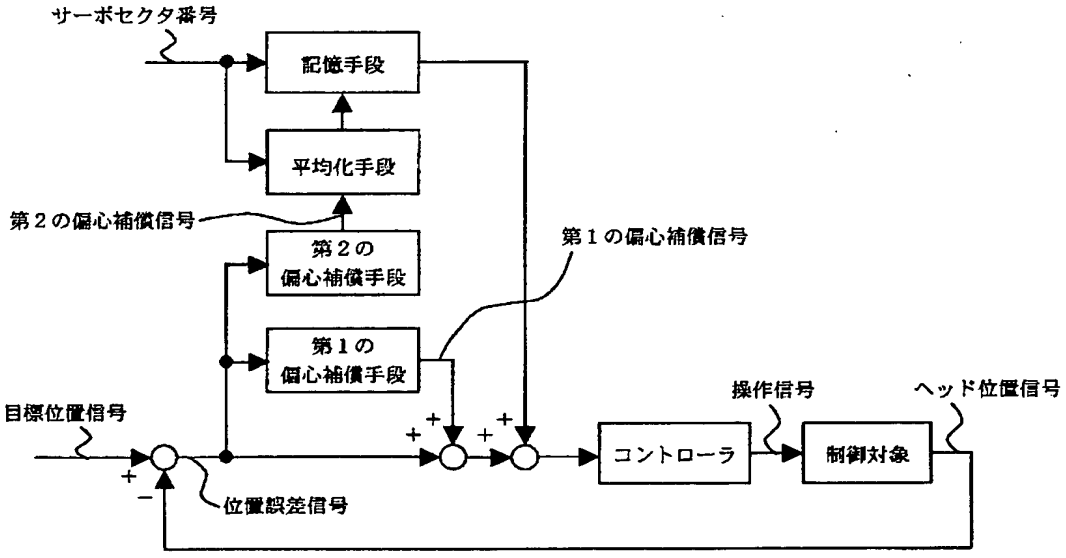
【図４】

図４


開始
認証鍵作成のコマンド入力あり？
NO
２００
YES
２０１
認証鍵作成
２０２
ホストシステム１０１に認証鍵送信
２０３
認証鍵記録手段１４に記録
終了

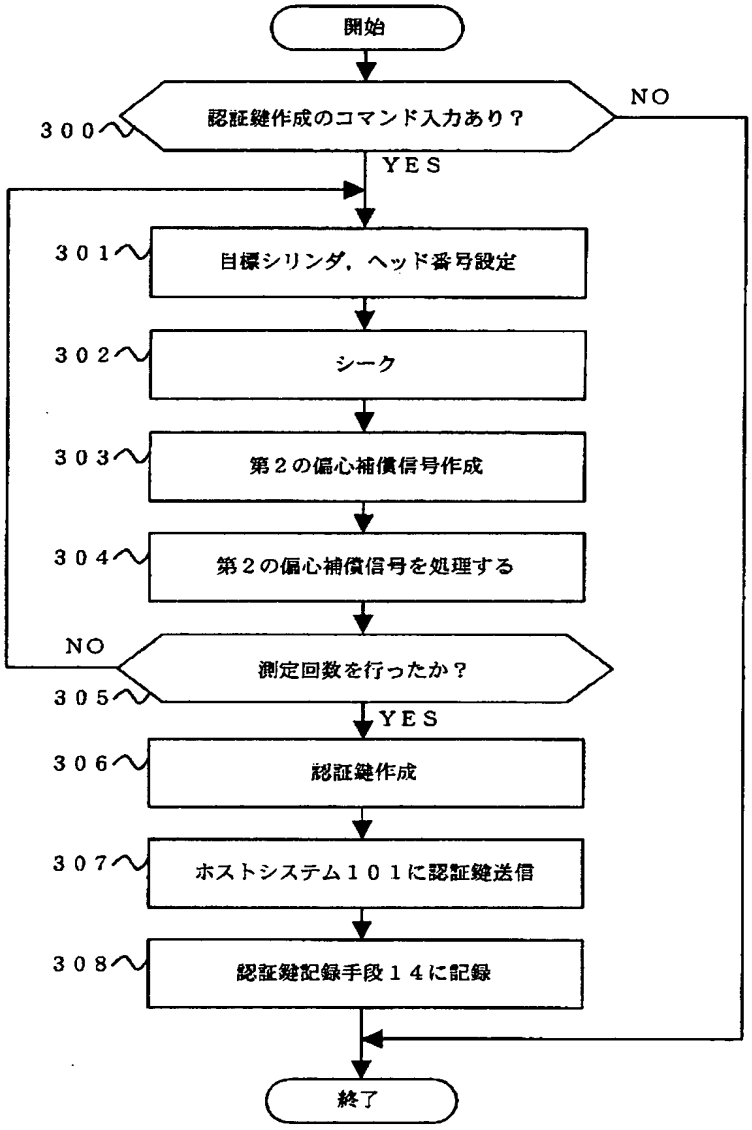
【図５】

図５


サーボセクタ番号
記憶手段
平均化手段
第２の偏心補償信号
第２の
偏心補償手段
第１の偏心補償信号
第１の
偏心補償手段
目標位置信号
操作信号
ヘッド位置信号
コントローラ
制御対象
位置誤差信号

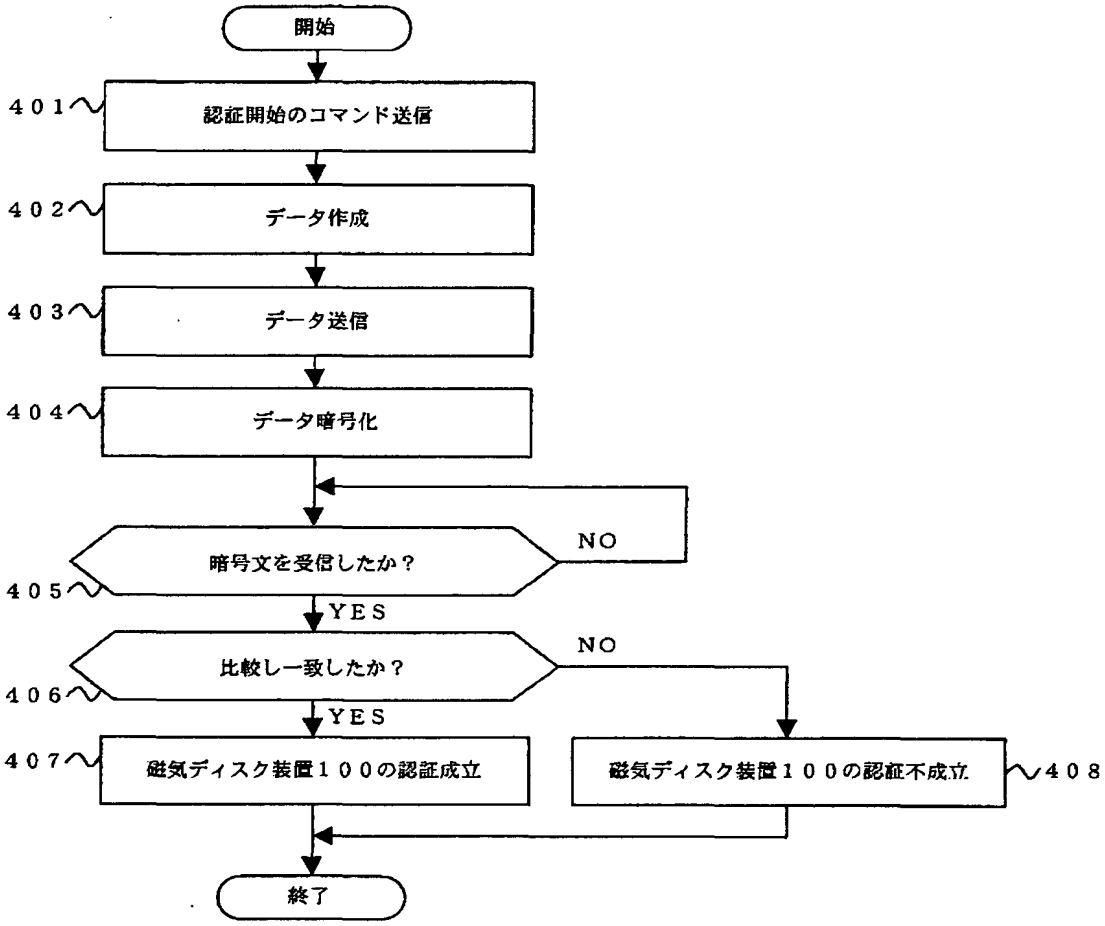
【図６】

図６


開始
300
認証鍵作成のコマンド入力あり？
NO
YES
301
目標シリンダ，ヘッド番号設定
302
シーク
303
第２の偏心補償信号作成
304
第２の偏心補償信号を処理する
NO
測定回数を行ったか？
305
YES
306
認証鍵作成
307
ホストシステム１０１に認証鍵送信
308
認証鍵記録手段１４に記録
終了

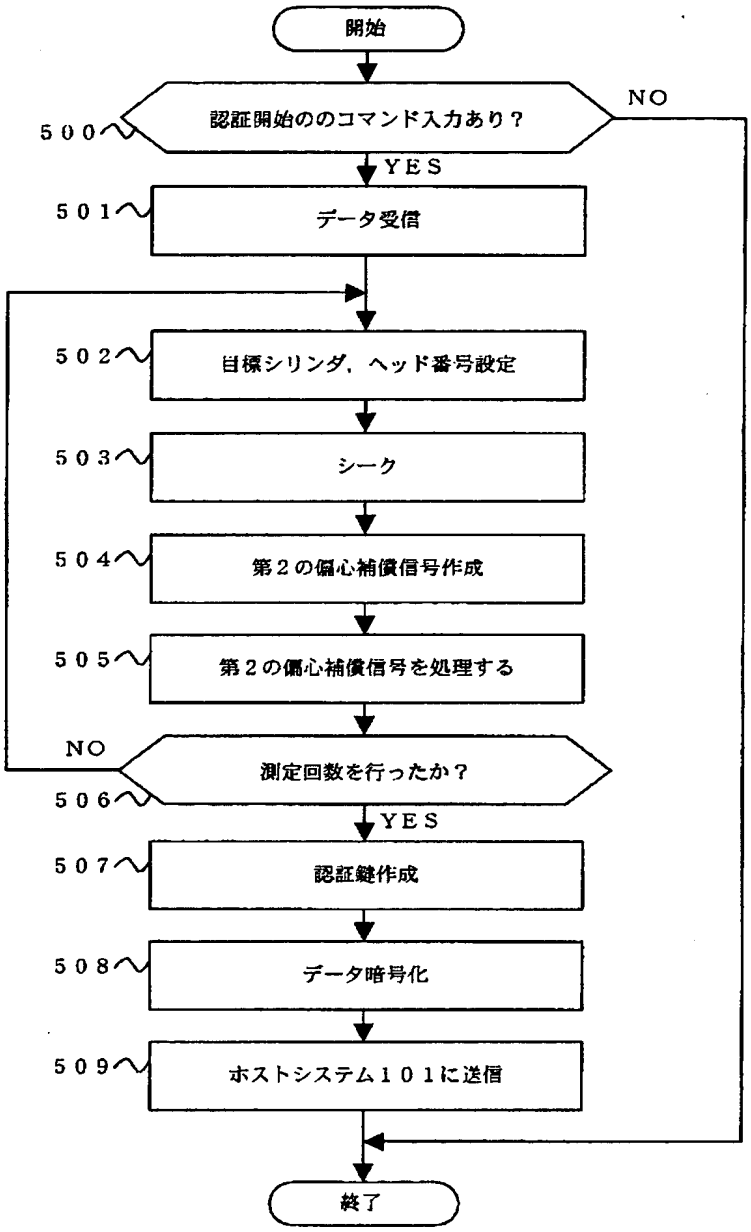
【図７】

図７


開始
４０１
認証開始のコマンド送信
４０２
データ作成
４０３
データ送信
４０４
データ暗号化
暗号文を受信したか？
NO
４０５
YES
比較し一致したか？
NO
４０６
YES
４０７
磁気ディスク装置１００の認証成立
磁気ディスク装置１００の認証不成立
４０８
終了

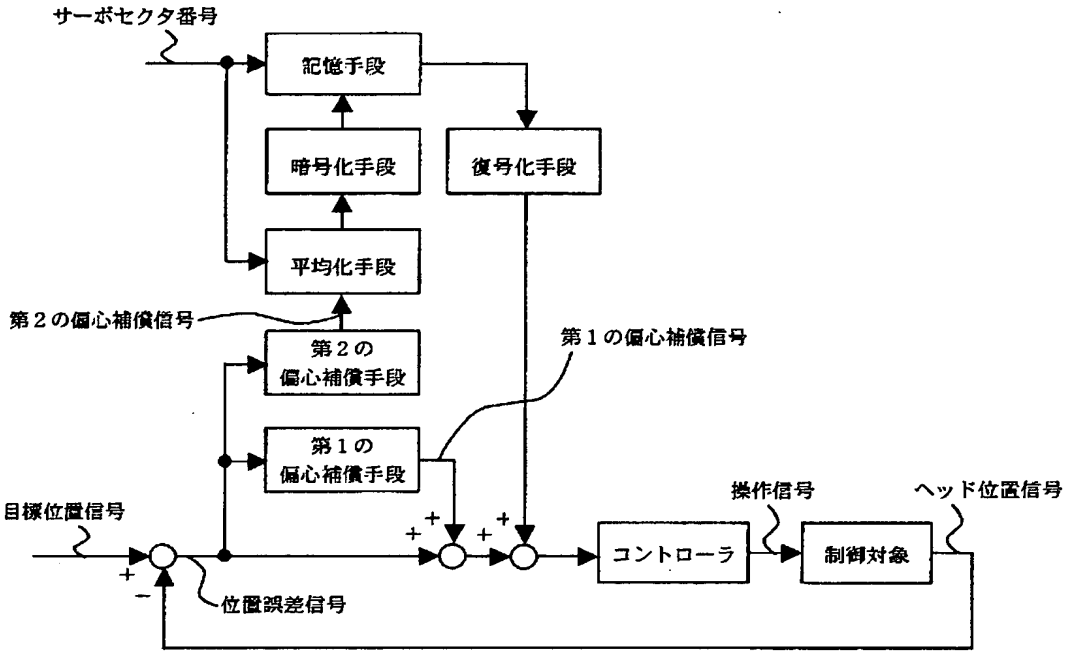
【図８】

図８


開始
500
認証開始ののコマンド入力あり？
NO
YES
501
データ受信
502
目標シリンダ，ヘッド番号設定
503
シーク
504
第２の偏心補償信号作成
505
第２の偏心補償信号を処理する
NO
測定回数を行ったか？
506
YES
507
認証鍵作成
508
データ暗号化
509
ホストシステム１０１に送信
終了

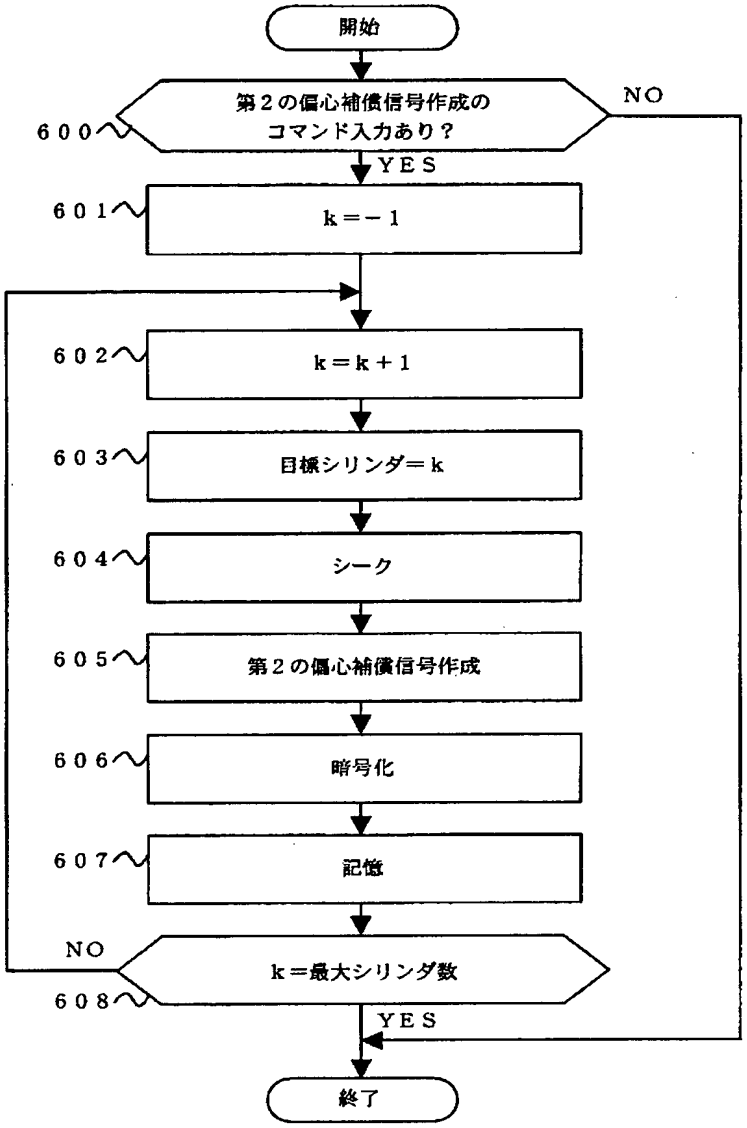
【図９】

図９


サーボセクタ番号
記憶手段
暗号化手段
復号化手段
平均化手段
第２の偏心補償信号
第２の
偏心補償手段
第１の偏心補償信号
第１の
偏心補償手段
目標位置信号
操作信号
ヘッド位置信号
コントローラ
制御対象
位置誤差信号

【図１０】

図１０


開始
第２の偏心補償信号作成の
コマンド入力あり？
NO
６００
YES
６０１
k＝－１
６０２
k＝k＋１
６０３
目標シリンダ＝k
６０４
シーク
６０５
第２の偏心補償信号作成
６０６
暗号化
６０７
記憶
NO
k＝最大シリンダ数
６０８
YES
終了

【書類名】　要約書

【要約】

【課題】

磁気ディスク装置にアクセスするホストシステムを特定のものに限定可能とする情報記録再生システムを提供する。

【解決手段】

磁気ディスク装置１００は、自身の物理的な特性に基づき認証鍵を作成する認証鍵作成手段１３を有し、磁気ディスク装置１００及びホストシステム１０１は、認証鍵を記録する認証鍵記録手段１４と認証鍵に基づき認証データを作成する認証データ作成手段１５とをそれぞれ有し、ホストシステム１０１の認証データと、磁気ディスク装置１００の認証データとに基づいて、ホストシステム１０１からの磁気ディスク装置１００の情報へのアクセスを制御する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－１８２３２５
受付番号	５０２００９１２３６６
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年　６月２５日

＜認定情報・付加情報＞

【提出日】　平成14年 6月24日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所